MURF.AI

Security at Murf

AICPA SOC aicpa.org/soc4so SOC for Service Organizations: Service Organizations

ISO 45001:2018 BQSR IAS ACCREDITED CERTIFIED

GDPR COMPLIANT

Safeguarding the Murf Platform

Architecture and Data Segregation

Murf operates as a multi-tenant software-as-a-service (SaaS) platform, utilizing a shared infrastructure to deliver a seamless experience for all users. To ensure customer data remains logically separated, we implement strict access controls and data isolation measures. Each customer's data is associated with a unique identifier, and access is managed through predefined access lists, preventing unauthorized cross-tenant access. These safeguards ensure that while our platform remains scalable and efficient, your data remains private and secure within its designated environment.

Cloud Infrastructure

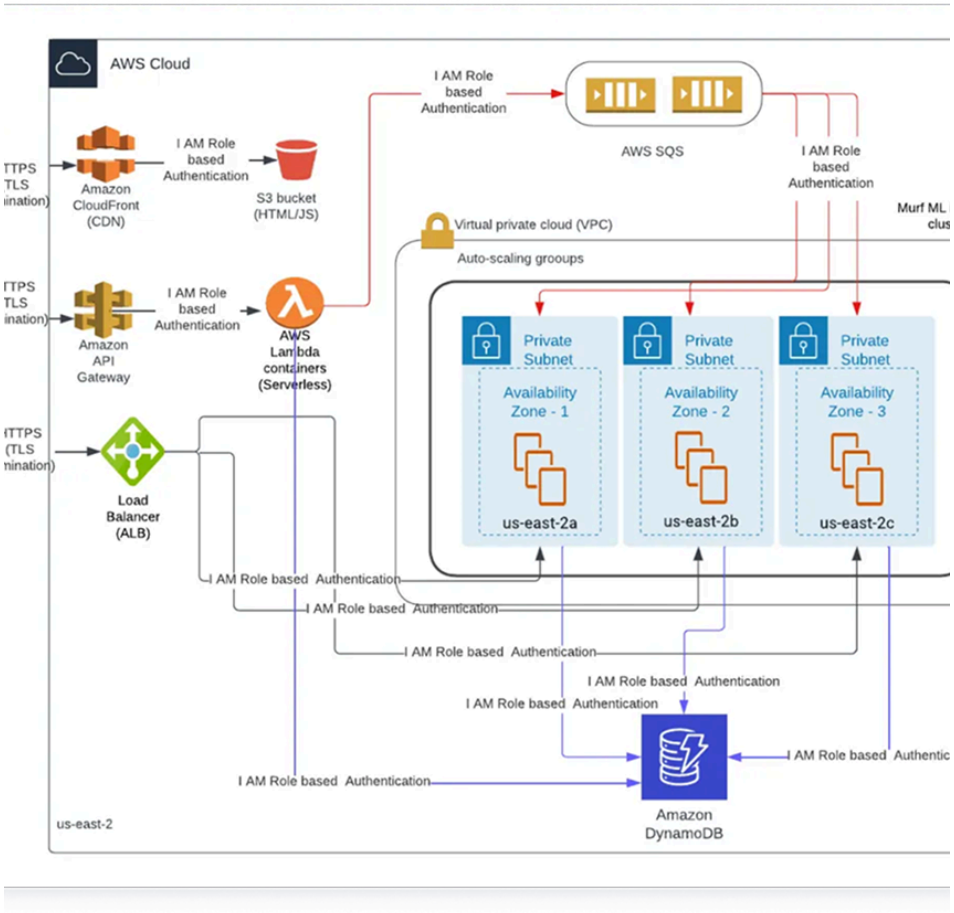
Murf is hosted on Amazon Web Services (AWS) in the United States, leveraging its secure and scalable cloud infrastructure**.** AWS powers key components of our platform, including web hosting, user management, backend APIs, compute resources, databases, monitoring, and automation. We make extensive use of AWS services to deliver a performant and resilient experience. Our machine learning models run securely within a Virtual Private Cloud (VPC), and we utilize AWS Identity and Access Management (IAM) to enforce strict, least-privilege access controls across our environment.

ML Inference Infrastructure

To support high-scale, low-latency speech synthesis, Murf operates dedicated clusters of high-configuration EC2 instances to run our machine learning models. These compute clusters are replicated across three availability zones within the US-East-2 (Ohio) region for enhanced resiliency and fault tolerance.

Dynamic auto-scaling is enabled to seamlessly handle variable workloads while maintaining performance, ensuring that users experience reliable service even during peak demand.

Murf operates entirely within a secure AWS cloud environment, using isolated infrastructure and best-practice security configurations. While we currently run on a public cloud architecture, we remain open to exploring private or hybrid cloud options as our platform evolves. This approach allows us to maintain high availability, reliability, and security while ensuring our infrastructure remains resilient and adaptable to evolving needs.



Murf AI’s Network Architecture

Encryption & Data Protection

Murf employs strong encryption protocols to safeguard customer data at all times. All stored customer data is encrypted on AWS using AES-256, a widely recognized industry standard for data security.

Encryption keys are securely managed using Amazon Key Management Service (KMS), which enforces periodic key rotation. Amazon KMS utilizes hardware security modules (HSMs) validated under FIPS 140-2, ensuring a high level of cryptographic security. By design, AWS employees and other unauthorized parties cannot access plaintext encryption keys.

All data transmitted between systems is encrypted in transit using TLS 1.2 to prevent unauthorized interception. Murf follows a formal cryptography policy, which defines encryption standards, key management practices, and security procedures to ensure ongoing data protection.

Data Residency

Murf securely stores and processes all Customer Data within the United States, leveraging Amazon Web Services (AWS) cloud infrastructure. All data is housed in AWS's US-East-2 region, located in Ohio, and all operational and backup storage remains within this region to ensure strict adherence to data residency requirements.

Storage & Backups

- Customer Data, including operational and backup storage, is kept within AWS data centers in Ohio (US-East-2) to ensure compliance with security, redundancy, and availability best practices. Murf does not replicate or store Customer Data outside of the US-East-2 region, maintaining strict data residency.
- AWS storage facilities operate across multiple availability zones within the region, providing geographic redundancy, high availability, and fault tolerance through separate physical locations with redundant power, networking, and connectivity.

Data Processing

- Audio processing for Murf’s AI-powered voice generation also occurs in Ohio (US-East-2) to maintain low latency and high performance.
- By keeping both data storage and processing within the same region, Murf optimizes efficiency, security, and compliance while minimizing unnecessary data transfers.
- Our Privacy Policy follows the EU-U.S. Data Privacy Framework (DPF) Principles for personal data transfers from the European Union and the United Kingdom, and the Swiss-U.S. DPF Principles for data transfers from Switzerland.

Reliability, Backup, and Business Continuity

Murf's resilient infrastructure is designed to maintain high availability, consistently delivering service uptime of over 99%. Secure backups also ensure business continuity in the event of disruptions.

Our platform is built on AWS (US-East-2), and has 3 availability zones to mitigate risks from hardware failures or natural disasters. Murf follows strict recovery objectives:

- Recovery Time Objective (RTO): Under 30 minutes for full system recovery.
- Recovery Point Objective (RPO): 30 minutes to minimize potential data loss.

To achieve these recovery targets, Murf's systems architecture team continuously monitors and tests our backup, failover, and recovery mechanisms. Our failover strategy follows a passive failover approach, combined with partial traffic routing via DNS, allowing for seamless transitions with zero downtime during planned failovers.

Murf ensures robust backup and recovery through AWS services:

- Amazon DynamoDB Point-in-Time Recovery (PITR) allows restoring backups to recovery points just seconds in the past, ensuring minimal data loss.
- AWS Backup for S3 enables point-in-time recovery, allowing efficient restoration of stored data.
- We perform daily backups of production databases, which include point-in-time recovery options and daily snapshots.
- All backups are encrypted, access-controlled, and stored securely using AWS services, following the principle of least privilege.

Murf's backup recovery and deployment processes are tested at least annually to validate their effectiveness. Our redundant architecture ensures that critical resources are distributed across geographically dispersed data centers, supporting continuous availability and minimizing service disruptions. Importantly, Murf has experienced no security incidents or data breaches till date, a reflection of our strong security posture and proactive risk management efforts.

Additionally, Murf maintains a business continuity and disaster recovery (BC/DR) plan, which is reviewed and tested annually to ensure our ability to respond effectively to unexpected incidents.

Compliance and Governance

Compliance and Data Protection

Murf is committed to safeguarding customer data and ensuring compliance with global privacy and security regulations. We are **SOC 2 Type II**, **ISO 27001**, **GDPR**, and **CCPA** compliant, and we undergo regular third-party audits to validate our security and privacy controls.

SOC 2 Type II Certification
We have successfully completed a System and Organization Controls (SOC) 2 Type II audit. Developed by the American Institute of Certified Public Accountants (AICPA), the SOC 2 information security audit provides a report on the examination of controls relevant to the trust services criteria categories covering security, availability, processing integrity, confidentiality, and privacy over a specified period. Murf's SOC 2 Type II report did not have any noted exceptions and was issued with a "clean" audit opinion from the auditors. This certification guarantees the effectiveness of our organization's security protocols and operational procedures.

ISO 27001 Certification
ISO/IEC 27001 is an international standard to manage information security. Murf is ISO 27001 certified which signifies a best-practice approach in managing information security by addressing people, processes, and technology.

California Consumer Privacy Act (CCPA)
We operate in compliance with the California Consumer Privacy Act (CCPA), ensuring your rights regarding the personal information we collect. For comprehensive information, please consult our CCPA Privacy Notice. To submit an information request, please contact us at legal@murf.ai.

GDPR
We value your privacy and your rights as a data subject and process all personal data in accordance with the principles of GDPR. We have also appointed local partners as our privacy representative and your point of contact. If you want to contact us via our representative, Prighter or make use of your data subject rights, please visit the following website.
https://prighter.com/q/14532374752

Enterprise Grade Security and Commitments

We implement industry-standard encryption (AES-256 for data at rest and TLS 1.2+ for data in transit) to protect all customer data. Access to customer information is strictly controlled and limited to authorized personnel based on job role and necessity.

To maintain ongoing compliance and detect potential threats, we log all critical security-relevant events—such as authentication attempts, privilege escalations, configuration changes, and admin activity. These logs are stored in a tamper-evident, immutable format, retained according to internal policy, and monitored continuously through automated alerting systems.

We also conduct regular audits of system activity and access controls to ensure traceability and accountability. Any anomalies or policy violations are investigated promptly.

Murf has a well-defined **Incident Management Procedure** in place. In the event of a security incident, our team follows a structured process for detection, containment, resolution, and post-incident analysis. Customers are notified in accordance with regulatory and contractual obligations.

Customer Data Rights (GDPR & CCPA)

As part of our commitment to privacy and compliance with GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), customers have several data rights, including:

- **Right to Access**: Customers can request a copy of the personal data we store about them.
- **Right to Rectification**: If any data is inaccurate or incomplete, customers can request corrections.
- **Right to Erasure (Right to Be Forgotten)**: Customers may request the deletion of their personal data, subject to legal and contractual obligations.
- **Right to Data Portability**: Customers can request to receive their data in a structured, commonly used format.
- **Right to Object & Restrict Processing**: Customers can opt out of certain data processing activities.

Murf provides clear processes for customers to exercise these rights. If a request is made, we respond in compliance with applicable legal timelines and requirements.

Subprocessors

Murf engages third-party entities (“Subprocessors”) to process Customer Data as part of our Services. A full list of our Sub-Processors, along with details on their processing activities is recorded. Here is Murf AI's Sub-Processor List.

We conduct compliance reviews of our Subprocessors to ensure they meet our security and privacy standards. Where required by applicable law, Murf also performs Transfer Impact Assessments (TIAs) for cross-border data transfers involving Customer Data.

Murf requires all Subprocessors to implement appropriate technical and organizational measures to safeguard Customer Data, ensuring compliance with relevant data protection laws.

Security Controls & Risk Management

Murf has a comprehensive security framework built around industry best practices, risk management principles, and well-defined security policies. Our approach is designed to ensure the confidentiality, integrity, and availability of customer data at every stage—whether it's being processed, transmitted, or stored.

Responsible AI Development & Lifecycle Management

At Murf, we recognize that building secure, ethical, and high-performing AI requires careful attention throughout the entire development lifecycle. Our AI lifecycle process is designed to ensure that security, privacy, performance, and compliance considerations are embedded from the earliest stages of product development through to deployment and ongoing monitoring.

Defining Requirements with Precision

Each new AI capability begins with well-defined, traceable requirements led by our Product team. During this phase, we ensure that only relevant, high-quality, and non-copyrighted data is considered for model training. Design and Engineering teams then translate these requirements into secure workflows and implementation plans. We apply strict version control, peer reviews, and secure coding practices to maintain traceability and reduce risks during the development stage.

Testing in Isolated Environments

Before deployment, all new features and model updates go through rigorous testing in a segregated staging environment. Quality assurance is handled by team members who are independent from the developers to maintain objectivity. Personally identifiable information (PII) is explicitly excluded from any testing data, further reducing privacy risk. Deployment to production follows a structured change management process, including peer-reviewed pull requests and formal approval workflows.

Specialized Model Development

Our machine learning models are developed with specific performance and safety goals in mind. Murf maintains multiple backbone models, each optimized for its primary use case—ranging from studio-grade user control and voice customization to dubbing-ready multilingual alignment and low-latency API integrations. Any potential ethical or operational risks encountered during development are flagged for review and mitigation by our Information Security Officer.

Ongoing Oversight and Monitoring

Post-deployment, our engineering and security teams continuously monitor infrastructure and model performance. We use automated tools to scan for code-level and network vulnerabilities and maintain strict isolation between development, staging, and production environments. This ongoing diligence allows us to evolve responsibly, maintain system integrity, and meet our customers' trust and safety expectations

Protecting Customer Data

Murf is committed to safeguarding customer data through robust security measures and compliance with global data protection regulations. Our data protection strategies include:

- **Data Encryption**: All customer data is encrypted both in transit and at rest using industry-standard encryption protocols.
- **Access Controls**: Only authorized personnel have access to customer data, and all access is logged and monitored.
- **Minimal Data Collection**: We only collect and retain customer data that is essential for providing our services.
- **Regular Security Assessments**: Our infrastructure is continuously evaluated for vulnerabilities and compliance risks.

Access Management

Murf uses the IAM Module on AWS to govern access to all critical systems. Access is granted based on approved requests and follows the principle of least privilege. We conduct quarterly access reviews for all employees, ensuring that only authorized personnel retain access.

Multi-Factor Authentication (MFA)

To protect Murf employee accounts, we enforce company-wide multi-factor authentication (MFA), ensuring an added layer of security against unauthorized access attempts.

Audit Logging & Monitoring

We log important user and administrative activities and monitor them for signs of suspicious behavior. Logging mechanisms help support access monitoring and overall security awareness.

Endpoint & Device Security

Murf utilizes an on-device application to monitor the presence of essential security controls on employee devices, including:

- Antivirus software to detect and prevent malware
- Disk encryption to protect stored data
- Screen locks to prevent unauthorized access
- Software update compliance to ensure systems are running the latest security patches

Network Security

Murf implements strict security measures for its network infrastructure, including:

- Multi-factor authentication (MFA) for access to critical servers and databases
- Our internal networks have Access Control Lists and are not accessible from the Internet.
- Encrypted communications using TLS 1.2 to protect data in transit

Cloud Security Monitoring

We continuously monitor our AWS (US-East-2) cloud infrastructure for misconfigurations, vulnerabilities, and patching requirements. We use AWS Inspector and GuardDuty to monitor risks in our environment and vulnerabilities in our workloads in real time.

Application Security

Security is embedded into our Software Development Lifecycle (SDLC) to minimize risks early in the development process. Our security measures include:

- Threat modeling & security reviews for new features and significant changes
- Static code analysis and software composition analysis to detect vulnerabilities before deployment
- Third-party penetration testing by security vendors every 6 months

Change Management

All application code changes at Murf go through a structured change management process to ensure they are necessary, secure, and beneficial to the platform. Development is performed entirely in-house, with source code maintained in AWS CodeCommit under strict version control. Our Software Development Life Cycle (SDLC) includes prioritizing deliverables, designing for scale and security, developing with built-in test cases, and undergoing peer reviews by engineers familiar with the system. Approved code is merged into a development branch and deployed to a staging environment for functional and non-functional testing by our QA team. Once testing is complete, release managers oversee deployment to production via AWS CodePipeline, with immediate post-deployment monitoring through system metrics and alarms to ensure operational stability.

This rigorous lifecycle ensures that every change is properly reviewed, tested, deployed, and monitored to maintain the security, reliability, and performance of the Murf platform.

Monitoring, Response & Lifecycle

Security Logs & Monitoring

We maintain logs of key system activities and monitor them for unusual behavior. Logs are stored securely and are periodically reviewed to support the detection of potential security issues.

Incident Management

Murf has a documented and structured Incident Response Plan to handle security incidents effectively. This plan is:

- Reviewed at least annually to ensure it remains effective and up to date.
- Communicated to relevant teams, ensuring a coordinated response in case of an incident.

Our incident response team actively monitors and investigates security, availability, and confidentiality-related incidents.

Should an incident occur, it would be logged in Murf's security incident register, where every action taken during the response process is documented and later reviewed to improve future response strategies.

In the event of an unauthorized disclosure of customer data, Murf notifies impacted customers without undue delay, in accordance with applicable legal and regulatory requirements.

Customer Data Lifecycle

Return of Customer Data

During an active subscription, customers can export generated audio files from Murf's platform by downloading them in MP3 or WAV format.
After a customer's agreement with Murf ends, we provide a grace period of up to 90 days during which customers can retrieve their previously generated audio files. After this period, the data may be permanently deleted in accordance with Murf's data retention policies.

Deletion of Customer Data

Customers have full control over the content they create on Murf and can request its deletion at any time.

- Upon receiving a deletion request, Customer Data is permanently removed from Murf's systems, including backups, with undue delay. However, complex cases may push this timeline to an upper limit of 90 days.
- If an account is terminated, customers can request the deletion of all stored data, and Murf will provide confirmation once the process is complete.
- If no explicit deletion request is made after account termination, data is automatically deleted within 90 days as part of Murf's standard data retention policy.
- Murf relies on AWS services for secure data erasure and adheres to AWS's physical security controls and disposal standards to ensure proper data deletion.

Personnel Practices

Murf maintains strict personnel security measures to ensure appropriate control and supervision over employees. This includes comprehensive hiring policies, background checks (where permitted by law), and job-specific security clearances.

All employees undergo information security and privacy training during onboarding, with mandatory annual security training to reinforce best practices. Employees must acknowledge and adhere to Murf's security policies, which cover:

- Mandatory use of strong passwords and multi-factor authentication (MFA) for enhanced account security.
- Role-based access control, following the principle of least privilege with a monitored approval process.
- Non-Disclosure Agreements (NDAs) or similar confidentiality agreements to safeguard proprietary and customer information.
- Annual security and privacy awareness training, including phishing simulations and policy refreshers.
- Immediate revocation of system access upon employment termination to prevent unauthorized access.
- Physical security measures, including controlled office access via key cards and surveillance monitoring.
- Audit logging of employee access to backend infrastructure to track and monitor activity.
- Threat detection through Amazon GuardDuty, which provides continuous monitoring for suspicious activity, unauthorized access attempts, and potential security threats.

These measures ensure that Murf personnel uphold the highest security standards to protect customer data and platform integrity.